AMENDMENTS TO THE CLAIMS WITH MARKINGS TO SHOW CHANGES MADE, AND LISTING OF ALL CLAIMS WITH PROPER IDENTIFIERS

1. (Currently amended) A method for securely providing event-relevant information about an industrial control alarm event occurring in a machine from an industrial controller controlling the machine to a specified remote receiver via a network ~~using an Internet-related protocol~~, comprising the steps of:

assigning a specific receiver to each specific industrial control alarm event occurring in the machine;

writing event-relevant information to a database in the controller controlling the machine, said event-relevant information including sensitive ~~event-relevant~~ information;

transmitting to the specified receiver in response to the alarm event a receiver-specific message indicating that the alarm event has occurred and not containing said sensitive ~~event-relevant~~ information; ~~and~~

accessing the event-relevant information ~~written to the database in the controller~~ via a Web server using a cryptographically protected communication protocol based on an Internet browser in response to the receiver-specific message; and

performing at least one of failure analysis or fault repair on the machine using ~~the~~ sensitive ~~event-relevant~~ information accessed using said cryptographically protected communication protocol.

2. (Previously presented) The method of claim 1, wherein the cryptographically protected communication protocol based on the Internet browser comprises a "Hypertext Transfer Protocol Security" protocol.

3. (Original) The method of claim 2, wherein the "Hypertext Transfer Protocol Security" protocol comprises a "Secure Socket Layer" protocol or a "Transport Layer Security" protocol.

4. (Previously presented) The method of claim 1, wherein the receiver-specific message is transmitted to the specified receiver as an e-mail message, an SMS message or a voice message.

5. (Previously presented) The method of claim 4, wherein the e-mail message includes a cross-reference, in particular a URL address, that provides a link to the event-relevant information that is stored in the database for the specified receiver.

6. (Previously presented) The method of claim 1, wherein the event-relevant information written to the database for the specified receiver includes file attachments which are stored in the database for the specified receiver.

7. (Original) The method of claim 1, wherein access to the Web server is protected by a login prompt and a password.

8. (Previously presented) The method of claim 1, wherein the Web server is integrated with hardware of the controller.

9. (Original) The method of claim 1, wherein at least one of the database and the Web server are implemented as hardware that is separate from hardware of the controller.

10. (Previously presented) The method of claim 1, further comprising the step of transmitting at least one of data, parameters and programs from the specified receiver to the controller.

11. (Currently amended) A method for securely providing event-relevant information about an industrial control alarm event occurring in a machine from an industrial controller controlling the machine to a specified remote receiver via a network ~~using an Internet-related protocol~~, comprising the steps of:

assigning a specific receiver to each specific industrial control alarm event occurring in the machine ;

writing event-relevant information to a database in the controller controlling the machine, said event-relevant information including sensitive ~~event-relevant~~ information;

transmitting to the specified receiver in response to the alarm event a receiver-specific message indicating that the alarm event has occurred and not containing said sensitive ~~event-relevant~~ information; ~~and~~

accessing the event-relevant information ~~written to the database in the controller~~ using a modem connection protected by an authentication protocol [[,]] in response to the receiver-specific message; and

performing at least one of failure analysis or fault repair on the machine using sensitive ~~event-relevant information~~ accessed using said protected modem connection ~~cryptographically protected communication protocol~~.

12. (Previously presented) The method of claim 1, wherein the event-relevant information written to the data base includes at least one of event messages, fault messages, information about machine status and process information, or a combination thereof.

13. (Cancelled)

14. (Previously presented) The method of claim 1, wherein only a receiver-specific message indicating that a specified alarm event has occurred is transmitted to the specified receiver.

15. (Previously presented) The method of claim 11, wherein the event-relevant information written to the data base includes at least one of event messages, fault messages, information about machine status and process information, or a combination thereof.

16. (Cancelled)

17. (Previously presented) The method of claim 11, wherein only a receiver-specific message indicating that a specified alarm event has occurred is transmitted to the specified receiver.

18. (Previously presented) The method of claim 11, further comprising the step of transmitting at least one of data, parameters and programs from the specified receiver to the controller.

19. (Previously presented) The method of claim 11, wherein the event-relevant information that is written to the database includes at least one of event messages, fault messages, information about machine status and process information, or a combination thereof.

20. (Previously presented) The method of claim 1, wherein only a receiver-specific message indicating that a specified alarm event has occurred is transmitted to the specified receiver.

21. (Previously presented) The method of claim 1 wherein the event-relevant information is written to a receiver-specific database element of the database.

22. (Previously presented) The method of claim 11 wherein the event-relevant information is written to a receiver-specific database element of the database.